

CLAIMS

The following listing of claims lists all of the pending claims, and supersedes all prior listings, and versions, of claims in this application.

LISTING OF CLAIMS:

1. (Currently amended) A method for authenticating a party to a transaction, the method comprising:
 - receiving a packet having at least a part of layer 2 header information replaced with a unique bit string;
 - examining at least a part of the unique bit string;
 - comparing the at least a part of the unique bit string examined with stored information; and
 - authenticating the party only if the at least a part of the unique bit string examined matches the stored information;
 - wherein the at least a part of the unique bit string examined depends on a type of the transaction, the type being a type of financial transaction.
2. (Previously presented) The method of claim 1 further comprising:
 - approving a transaction if the party was authenticated.
3. (Canceled)
4. (Original) The method of claim 2 wherein the stored information compared with the at least a part of the unique bit string examined depends on the type of the transaction.
5. (Original) The method of claim 3 wherein the type of the transaction is selected from a group of transaction types consisting of: (A) transactions greater than a predetermined amount; (B)

transactions less than a predetermined amount; (C) purchases delivered to a credit card billing address; and (D) purchases delivered to an address other than a credit card billing address.

6. (Original) The method of claim 1 wherein the stored information compared with the at least a part of the unique bit string examined depends on a type of the transaction.

7. (Original) The method of claim 1 wherein the at least a part of the unique bit string examined identifies a location at which packets from the party to the transaction entered the network.

8. (Original) The method of claim 1 wherein the at least a part of the unique bit string examined identifies an individual who is a party to the transaction.

9. (Original) The method of claim 1 wherein the at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs.

10. (Original) The method of claim 1 wherein the at least a part of the unique bit string examined identifies a customer that is a party to the transaction.

11. (Original) The method of claim 1 wherein the at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and a user class.

12. (Original) The method of claim 1 wherein the at least a part of the unique bit string identifies at least two of a customer identification, an individual user identification, a network ingress location, and a user class.

13. (Original) The method of claim 1 wherein the at least a part of the unique bit string identifies at least three of a customer identification, an individual user identification, a network ingress location, and a user class.
14. (Original) The method of claim 1 wherein the unique bit string is provisioned by a network service provider.
15. (Original) The method of claim 1 wherein the unique bit string is controlled by a network service provider.
16. (Original) The method of claim 1 wherein the act of authenticating does not require the transmission of any authentication information from the party.
17. (Previously presented) A method for tracking a network ingress location at which a packet associated with a transaction originated, the method comprising:
- receiving the packet, the packet having at least a part of layer 2 header information replaced with a unique bit string;
 - examining at least a part of the unique bit string; and
 - determining the network ingress location from the at least a part of the unique bit string.
18. (Original) The method of claim 17 wherein the at least a part of the unique bit string examined identifies an individual who is a party to the transaction.
19. (Original) The method of claim 17 wherein the at least a part of the unique bit string examined identifies a group to which an individual, who is a party to the transaction, belongs.
20. (Original) The method of claim 17 wherein the at least a part of the unique bit string examined identifies a customer that is a party to the transaction.

21. (Original) The method of claim 17 wherein the at least a part of the unique bit string identifies at least one of a customer identification, an individual user identification, a network ingress location, and an individual user class.
22. (Original) The method of claim 17 wherein the unique bit string is provisioned by a network service provider.
23. (Original) The method of claim 17 wherein the unique bit string is controlled by a network service provider.
24. (Previously presented) A method for authenticating a party to a transaction, the method comprising:
- receiving a packet having at least a part of layer 2 header information replaced with a unique bit string;
 - examining at least a part of the unique bit string;
 - comparing the at least a part of the unique bit string examined with stored information; and
 - approving a transaction only if the at least a part of the unique bit string examined matches the stored information,
- wherein the unique bit string uniquely identifies the party and an ingress location of the network, and no information in addition to the unique bit string is needed for authenticating the party to the transaction.
25. (Cancelled)
26. (Original) The method of claim 24 wherein the unique bit string is maintained as the packet is communicated within the network.

27. (Previously presented) The method of claim 24 wherein the unique bit string identifies a logical port at which the packet entered the network.

28. (Currently amended) A method for authenticating a party to a transaction, the method comprising:

a) applying a unique bit string to layer 2 header information of packets entering the network, the unique bit string uniquely identifying the party and an ingress location of the network;

b) examining at least a part of the unique bit string;

c) comparing the at least a part of the unique bit string examined with stored information;

and

d) approving a transaction only if the at least a part of the unique bit string examined matches the stored information;

wherein the at least a part of the unique bit string examined depends on a type of the transaction, the type being a type of financial transaction.

29. (Cancelled)

30. (Original) The method of claim 28 wherein the unique bit string is maintained as the packet is communicated within the network.

31. (Original) The method of claim 28 wherein the unique bit string identifies a logical port at which the packet entered the network.

32. (Original) The method of claim 28 wherein no information in addition to the unique bit string is needed for authenticating the party to the transaction.

33. (Currently amended) An apparatus for authenticating a party to a transaction, the apparatus comprising:

a) an input for accepting an authentication request, the authentication request including a packet having at least a part of a layer 2 header information replaced with a unique bit string;

b) storage means for storing authentication information;

c) means for examining at least a part of the unique bit string;

d) a comparison facility for comparing the at least a part of the unique bit string examined with the stored authentication information; and

e) means for authenticating a party to a transaction only if the at least a part of the unique bit string examined matches the stored authentication information;

wherein the at least a part of the unique bit string examined depends on a type of the transaction, the type being a type of financial transaction.

34. (Original) The apparatus of claim 33 further comprising:

f) means for approving the transaction if the party was authenticated.

35. (Original) The apparatus of claim 33 further comprising:

f) an output for forwarding an authentication response to the transaction facility.

36. (Original) The apparatus of claim 34 further comprising:

g) an output for forwarding an authorization response to the transaction facility.

37. (Previously presented) The method of claim 1, wherein the layer 2 header information is one of data link layer header and a network access layer header.

38. (Previously presented) The method of claim 17, wherein the layer 2 header information is a MAC header.